



US
Jc879 U.S. PTO
10/084755
02/25/02

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

17 OCT. 2001

Fait à Paris, le

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (1) 53 04 53 04
Télécopie : 33 (1) 42 93 59 30
www.inpi.fr

This Page Blank (uspto)

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W /260899

REMISE DES PIÈCES DATE 27 FEV 2001 LIEU 75 INPI PARIS N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0102664 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 27 FEV. 2001		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE Christophe SAINT-MARC Société Civile SPID 156 boulevard Haussmann 75008 PARIS	
Vos références pour ce dossier (facultatif) PHFR010022			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N°	Date / /
		N°	Date / /
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/>	
		N°	Date / /
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Système de réception de signaux cryptés multi-opérateurs à encombrement et coût réduits			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date / / N° Pays ou organisation Date / / N° Pays ou organisation Date / / N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		Koninklijke Philips Electronics N.V.	
Prénoms			
Forme juridique		Société de droit néerlandais	
N° SIREN			
Code APE-NAF			
Adresse	Rue	Groenewoudseweg 1	
	Code postal et ville	5621 BA Eindhoven	
Pays		Pays-Bas	
Nationalité			
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

Réservé à l'INPI

REMISE DES PIÈCES

DATE

27 FEV 2001

LIEU

75 INPI PARIS

N° D'ENREGISTREMENT

NATIONAL ATTRIBUÉ PAR L'INPI

0102664

_DB 540 W / 260899

Vos références pour ce dossier :*(facultatif)***PHFR010022****6 MANDATAIRE**

Nom

SAINT-MARC

Prénom

Christophe

Cabinet ou Société

Société Civile SPIDN° de pouvoir permanent et/ou
de lien contractuel**pouvoir général n° 7036 délégation de pouvoir n° 9363**

Adresse

Rue

156 boulevard Haussmann

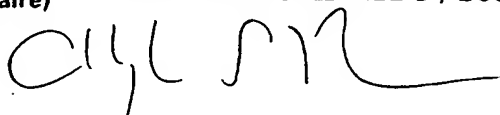
Code postal et ville

75008 PARISN° de téléphone *(facultatif)***01 40 76 80 00**N° de télécopie *(facultatif)***01 45 61 05 36**Adresse électronique *(facultatif)***7 INVENTEUR (S)**

Les inventeurs sont les demandeurs

☐ Oui☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée****8 RAPPORT DE RECHERCHE****Uniquement pour une demande de brevet (y compris division et transformation)**Établissement immédiat
ou établissement différé☒☐

Paiement échelonné de la redevance

Paiement en trois versements, uniquement pour les personnes physiques☐ Oui☐ Non**9 RÉDUCTION DU TAUX
DES REDEVANCES****Uniquement pour les personnes physiques**☐ Requête pour la première fois pour cette invention *(joindre un avis de non-imposition)*☐ Requête antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):*Si vous avez utilisé l'imprimé «Suite»,
indiquez le nombre de pages jointes**10 SIGNATURE DU DEMANDEUR
OU DU MANDATAIRE**
(Nom et qualité du signataire)**Christophe Saint-Marc****Mandataire SPID 422-5 / S008**

**VISA DE LA PRÉFECTURE
OU DE L'INPI**


La présente invention concerne un système destiné à opérer une réception de signaux de données encodés et cryptés, et un traitement desdits signaux afin de les convertir en stimuli de sortie compréhensibles par un utilisateur dudit système.

De tels systèmes sont couramment utilisés dans l'industrie électronique pour, entre autres, capter et visualiser des programmes de télévision numérique. Les systèmes actuels incluent généralement :

- . un décodeur,
- . des moyens de décryptage, et
- . un dispositif de sortie, par exemple un téléviseur ou un moniteur, pour produire les stimuli de sortie, en l'occurrence des images et des sons, sur la base de signaux de sortie du décodeur.

Dans l'état actuel du marché des programmes de télévision numérique, formés par des ensembles de signaux de données, et du matériel y afférent, lesdits programmes sont encodés selon des standards de compression de données audiovisuelles de type MPEG. Chaque émetteur de signaux de données, communément appelé opérateur, conçoit un décodeur spécifiquement étudié pour décrypter et décoder, c'est-à-dire décompresser, ses propres programmes, ce qui entraîne que le décodeur est contenu dans un boîtier dans lequel sont le plus souvent inclus les moyens de décryptage. Un tel décodeur est incapable de décrypter et par conséquent de décoder des programmes provenant d'un autre opérateur. Un utilisateur qui souhaite recevoir des programmes en provenance de plusieurs opérateurs différents devra donc se munir d'autant de boîtiers-décodeurs différents, ce qui engendre un coût et un encombrement importants du système multi-opérateurs ainsi créé.

L'un des buts de la présente invention est de permettre à un utilisateur de recevoir des programmes provenant de différents opérateurs, sans pour autant que le système utilisé à cet effet ne présente les inconvénients décrits ci-dessus.

En effet, selon l'invention, le décodeur et les moyens de décryptage inclus dans le système conforme au paragraphe introductif peuvent être incorporés dans le dispositif de sortie, le système comportant en outre des moyens d'autorisation, destinés à recevoir, de la part d'un émetteur de signaux de données, des informations sécurisées, et à fournir un signal d'autorisation consécutivement à la réception desdites informations, lequel signal d'autorisation est destiné à activer les moyens de décryptage.

Dans un tel système, les moyens de décryptage ne décryptent effectivement les signaux de données que lorsqu'ils y sont autorisés par l'émetteur desdits signaux, c'est-à-dire, le plus souvent, après que l'utilisateur du système aura conclu une transaction avec l'opérateur correspondant.

Plusieurs hypothèses de fonctionnement sont envisageables :

Les moyens de décryptage peuvent contenir un logiciel de décryptage standard pour tous les programmes susceptibles d'être reçus par le système, le décryptage de chaque programme n'étant possible que grâce à une clé spécifique à ce programme, définie par l'opérateur qui est

l'émetteur dudit programme. Dans une telle hypothèse de fonctionnement, la clé pourra constituer le signal d'autorisation.

Dans cette hypothèse, des signaux de données décryptés seront disponibles en sortie des moyens de décryptage si ceux-ci sont inclus dans un module autonome, et risqueront d'être
5 interceptés par un utilisateur mal intentionné aux fins de recopie illégale du contenu du programme décodé.

Il est donc souhaitable de prévoir des aménagements empêchant que l'utilisateur du système ne puisse avoir accès aux signaux décryptés.

A cet effet, les moyens de décryptage seront avantageusement inclus dans le
10 décodeur.

Si, de surcroît, le décodeur est lui-même inclus dans le dispositif de sortie, les seules informations qui seront directement accessibles à l'utilisateur seront les informations sécurisées fournies par l'émetteur des signaux de données, ce qui limite les risques de contrefaçon du contenu des programmes reçus par le système.

15 Dans une autre hypothèse de fonctionnement, les moyens de décryptage peuvent contenir des moyens matériels pour exécuter un logiciel de décryptage, sans pour autant contenir le logiciel lui-même, auquel cas le dit logiciel sera acheminé, au moyen du signal d'autorisation, vers les moyens de décryptage où il sera mémorisé. Un tel acheminement sera assujéti à la réception par les moyens d'autorisation des informations sécurisées, qui pourront
20 contenir un code définissant le logiciel de décryptage. Dans cette autre hypothèse, on pourra prévoir d'incorporer les moyens d'autorisation au décodeur, intégré ou non dans le dispositif de sortie, ce qui empêchera que le logiciel de décryptage ne soit directement accessible à l'utilisateur du système, et limitera les risques de contrefaçon du contenu des programmes. Un tel mode de réalisation de l'invention permet en outre de réduire encore l'encombrement du
25 système.

Selon un mode de réalisation particulier de l'invention, le décodeur est muni d'une interface pour permettre des échanges de données avec des appareils périphériques au dispositif de sortie, le signal d'autorisation étant destiné à être acheminé depuis les moyens d'autorisation vers les moyens de décryptage via ladite interface.

30 Un tel mode de réalisation tire parti du fait que la plupart des décodeurs devront, dans un proche avenir, être munis d'une interface standard, par exemple du type USB, et permettra donc d'utiliser des ressources préexistantes pour l'acheminement du signal d'autorisation.

Selon un mode de mise en œuvre de l'invention, les moyens d'autorisation
35 contiennent une mémoire dans laquelle sont stockées les informations sécurisées.

Dans ce mode de mise en œuvre, chaque opérateur doit fournir les moyens d'autorisation qui lui sont spécifiques, destinés à être connectés au dispositif de sortie. L'encombrement résultant pour le système est cependant moins important que dans les

systèmes multi-opérateurs connus, les moyens d'autorisation qui seront ici essentiellement constitués par une mémoire et un connecteur associé, étant moins volumineux qu'un boîtier-décodeur.

5 Dans un autre mode de mise en œuvre de l'invention, les moyens d'autorisation incluent un lecteur de support mémoire amovible, les informations sécurisées étant destinées à être stockées dans la mémoire dudit support.

Ce mode de mise en œuvre permet de limiter encore l'encombrement et le coût du système, puisqu'un seul lecteur est nécessaire, l'adaptation du système aux contraintes d'un nouvel opérateur se faisant par simple changement de support mémoire amovible.

10 On pourra en outre munir les moyens d'autorisation d'une pluralité de connecteurs, chacun destiné à recevoir un support mémoire amovible fourni par un opérateur.

Les supports mémoire amovibles peuvent revêtir différentes formes, et seront avantageusement constitués par des bâtonnets mémoire ou des cartes à puce.

15 Une variante de l'invention, selon laquelle les moyens d'autorisation sont munis d'un modem permettant d'établir un échange de données en temps réel entre le système et un émetteur de signaux de données, est avantageuse en ce qu'elle autorise, outre un téléchargement des informations sécurisées par l'opérateur émetteur des signaux de données, une communication bidirectionnelle entre l'utilisateur et différents opérateurs, qui permettra par exemple des transactions, notamment dans des applications de télévision à péage ou de
20 téléachat.

Bien que le système décrit jusqu'à présent soit un système de télévision, l'invention n'est en aucun cas limitée à cette seule application. L'invention pourra par exemple être utilisée dans le cadre de la réception conditionnelle de programmes radiophoniques, ou encore dans celui de télécommunications sécurisées, où les stimuli de sortie seront exclusivement sonores.

25 Dans un de ses modes de mise en œuvre, l'invention concerne également un procédé pour décrypter et décoder des signaux de données au sein d'un système destiné à convertir lesdits signaux en stimuli de sortie compréhensibles par un utilisateur dudit système, procédé incluant une étape d'acheminement d'un logiciel de décryptage, vers des moyens de décryptage contenant des moyens matériels pour exécuter ledit logiciel, depuis des moyens
30 d'autorisation destinés à recevoir des informations sécurisées de la part d'un émetteur des signaux de données.

L'invention sera mieux comprise à l'aide de la description suivante, faite à titre d'exemple non-limitatif et en regard des dessins annexés, dans lesquels :

- 35 - la figure 1 est un schéma fonctionnel décrivant un système de réception conforme à un mode de mise en œuvre de l'invention, et
- la figure 2 est un schéma fonctionnel décrivant un système de réception conforme à une variante particulièrement avantageuse de ce mode de mise en œuvre de l'invention.

La figure 1 représente schématiquement un système SYST destiné à recevoir, depuis une antenne ANT, des signaux de données DS encodés et cryptés, et à opérer un traitement desdits signaux DS afin de les convertir en stimuli de sortie compréhensibles par un utilisateur dudit système SYST, incluant :

- 5 . un dispositif de sortie DISP, incluant un décodeur DEC des signaux de données DS, et muni de moyens pour produire les stimuli de sortie sur la base de signaux de sortie OS du décodeur DEC,
- . des moyens de décryptage DES pour décrypter les signaux de données DES, lesdits moyens étant inclus dans le dispositif de sortie DISP et destinés à être activés par un signal
- 10 d'autorisation ES,
- . des moyens d'autorisation EN, destinés à recevoir des informations sécurisées de la part d'un émetteur des signaux de données, et à fournir le signal d'autorisation ES consécutivement à la réception desdites informations.

Dans l'exemple décrit ici, le dispositif de sortie est muni de moyens d'affichage, 15 comme par exemple un tube cathodique, ou encore un écran à cristaux liquides ou à plasma, les stimuli de sortie étant des images et des sons. Les signaux de sortie OS du décodeur DEC seront utilisés pour piloter lesdits moyens d'affichage.

Dans un tel système, les moyens de décryptage DES ne décryptent effectivement les signaux de données DS que lorsqu'ils y sont autorisés par l'émetteur desdits signaux, c'est-à-dire, le plus 20 souvent, après que l'utilisateur du système SYST aura conclu une transaction avec l'opérateur correspondant, qui aura alors livré à l'utilisateur les informations sécurisées.

Les moyens de décryptage DES peuvent contenir un logiciel de décryptage standard pour tous les programmes susceptibles d'être reçus par le système SYST, le décryptage de chaque programme n'étant possible que grâce à une clé spécifique à ce programme, définie par 25 l'opérateur qui est l'émetteur dudit programme. Dans une telle hypothèse, la clé pourra être contenue dans les informations sécurisées et constituer le signal d'autorisation ES.

Dans une autre hypothèse, les moyens de décryptage DES peuvent contenir des moyens matériels pour exécuter un logiciel de décryptage, sans pour autant contenir le logiciel lui-même, auquel cas le dit logiciel sera acheminé, au moyen du signal d'autorisation ES, vers les 30 moyens de décryptage DES où il sera mémorisé. Un tel acheminement sera assujéti à la réception des informations sécurisées par les moyens d'autorisation EN.

Ces informations sécurisées pourront contenir un code définissant le logiciel de décryptage. Selon le mode de réalisation particulier de l'invention décrit ici, les moyens de décryptage DES sont inclus dans le décodeur DEC, qui est muni d'une interface INT pour permettre des 35 échanges de données avec des appareils périphériques au dispositif de sortie DISP, le signal d'autorisation ES étant destiné à être acheminé depuis les moyens d'autorisation EN vers les moyens de décryptage DES via ladite interface INT.

Ce mode de réalisation tire parti du fait que la plupart des décodeurs devront, dans un proche

avenir, être munis d'une interface standard, par exemple du type USB ou IEEE1394, et permettra donc d'utiliser des ressources préexistantes pour l'acheminement du signal d'autorisation ES.

5 Les moyens d'autorisation EN incluent ainsi un lecteur de carte à puce SC, ladite carte étant fournie par un opérateur après que l'utilisateur du système SYST ait conclu une transaction avec ledit opérateur, ladite carte SC étant porteuse d'une mémoire dans laquelle les informations sécurisées sont destinées à être stockées.

Ainsi, lorsque l'utilisateur souhaitera accéder à des programmes d'un nouvel opérateur, il lui suffira d'insérer une nouvelle carte à puce correspondante dans les moyens d'autorisation EN. Il
10 apparaît clairement que l'invention permet une réduction considérable de l'encombrement et du coût du système SYST, puisque, dans l'état actuel de la technique, un utilisateur qui souhaite recevoir des programmes en provenance de plusieurs opérateurs différents doit se munir d'autant de boîtiers-décodeurs différents, l'invention ne nécessitant à cet effet, dans l'exemple décrit ici, qu'un seul lecteur de carte à puce et un jeu de cartes à puces fournies par lesdits
15 opérateurs.

Dans le système SYST décrit par la présente figure, les moyens d'autorisation EN sont munis d'un modem MD permettant d'établir, via une ligne téléphonique TEL, un échange de données en temps réel entre le système SYST et un émetteur de signaux de données. Cette variante de l'invention est avantageuse en ce qu'elle autorise un téléchargement d'informations sécurisées
20 par un opérateur, par exemple à des fins de mise à jour, mais aussi une communication bidirectionnelle entre l'utilisateur et différents opérateurs, qui permettra par exemple des transactions, notamment dans des applications de télévision à péage ou de téléachat.

La figure 2 représente schématiquement une variante du système SYST décrit ci-dessus. Les éléments communs avec la figure précédente sont munis des mêmes signes de
25 référence, et ne seront pas à nouveau décrits ici. Selon la présente variante, les moyens d'autorisation EN sont incorporés dans le dispositif de sortie DISP, lequel présente alors un connecteur destiné à recevoir le support contenant les informations sécurisées, par exemple une carte à puce SC, et un connecteur destiné à relier le modem MD avec une ligne téléphonique TEL.

30 Cette variante permet de limiter encore l'encombrement du système SYST, et présente en outre l'avantage suivant :

Dans l'hypothèse où le logiciel de décryptage est acheminé depuis les moyens d'autorisation EN vers les moyens de décryptage DES via le signal d'autorisation ES, ledit logiciel est pleinement opérationnel et risque d'être intercepté par un utilisateur mal intentionné aux fins de recopie
35 illégale du contenu du programme décodé.

La variante de l'invention décrite ici empêche que l'utilisateur du système SYST ne puisse avoir directement accès au logiciel de décryptage. Du fait que les moyens d'autorisation EN sont inclus dans le dispositif de sortie DISP, les seules informations qui seront directement

accessibles à l'utilisateur depuis l'extérieur dudit dispositif seront les informations sécurisées fournies par l'émetteur des signaux de données, ce qui limite les risques de contrefaçon du contenu des programmes reçus par le système.

- 5 En vue de limiter le coût du dispositif de sortie DISP, et de permettre des remplacements du modem MD par des versions améliorées tout au long de la durée de vie du dispositif de sortie DISP, on pourra choisir de dissocier des moyens d'autorisation EN le modem MD, qui constituera alors un appareil périphérique externe audit dispositif DISP.

REVENDEICATIONS

1. Système destiné à opérer une réception de signaux de données encodés et cryptés, et un traitement desdits signaux afin de les convertir en stimuli de sortie compréhensibles par un utilisateur dudit système, incluant :
 - 5 . un décodeur des signaux de données,
 - . un dispositif de sortie muni de moyens pour produire les stimuli de sortie sur la base de signaux de sortie du décodeur,
 - . des moyens de décryptage pour décrypter les signaux de données, lesdits moyens étant destinés à être activés par un signal d'autorisation,
 - 10 . des moyens d'autorisation, destinés à recevoir des informations sécurisées de la part d'un émetteur des signaux de données, et à fournir le signal d'autorisation consécutivement à la réception desdites informations.
2. Système selon la revendication 1, dans lequel les moyens de décryptage contiennent des moyens matériels pour exécuter un logiciel de décryptage, lequel logiciel étant
15 destiné à être acheminé vers les moyens de décryptage via le signal d'autorisation.
3. Système selon la revendication 1, dans lequel les moyens de décryptage sont inclus dans le décodeur.
4. Système selon la revendication 1, dans lequel les moyens d'autorisation sont incorporés dans le décodeur.
- 20 5. Système selon la revendication 1, dans lequel le décodeur est incorporé au dispositif de sortie.
6. Système selon la revendication 3, dans lequel le décodeur est muni d'une interface pour permettre des échanges de données avec des appareils périphériques, et dans lequel le signal d'autorisation est destiné à être acheminé depuis les moyens d'autorisation vers les
25 moyens de décryptage via ladite interface.

7. Système selon la revendication 1, dans lequel les moyens d'autorisation contiennent une mémoire dans laquelle sont stockées les informations sécurisées.
8. Système selon la revendication 1, dans lequel les moyens d'autorisation incluent un lecteur de support mémoire amovible, les informations sécurisées étant destinées à être
5 stockées dans la mémoire dudit support.
9. Système selon la revendication 8, dans lequel le support mémoire amovible est une carte à puce.
10. Système selon la revendication 1, dans lequel les moyens d'autorisation sont munis d'un modem permettant d'établir un échange de données en temps réel entre le système et un
10 émetteur de signaux de données.
11. Procédé pour décrypter et décoder des signaux de données au sein d'un système destiné à convertir lesdits signaux en stimuli de sortie compréhensibles par un utilisateur dudit système, procédé incluant une étape d'acheminement d'un logiciel de décryptage, vers des
15 moyens de décryptage contenant des moyens matériels pour exécuter ledit logiciel, depuis des moyens d'autorisation destinés à recevoir des informations sécurisées de la part d'un émetteur des signaux de données.

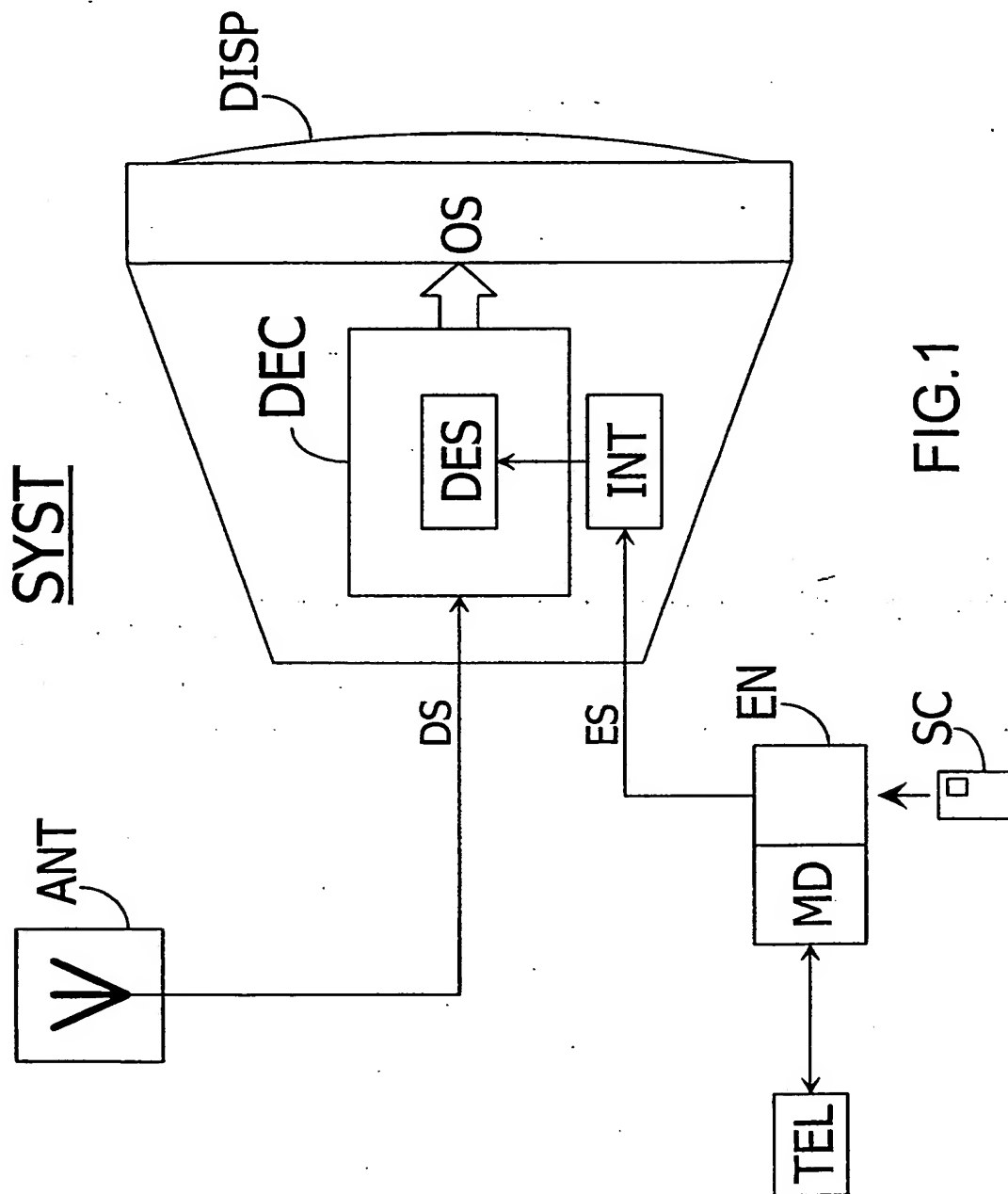


FIG.1

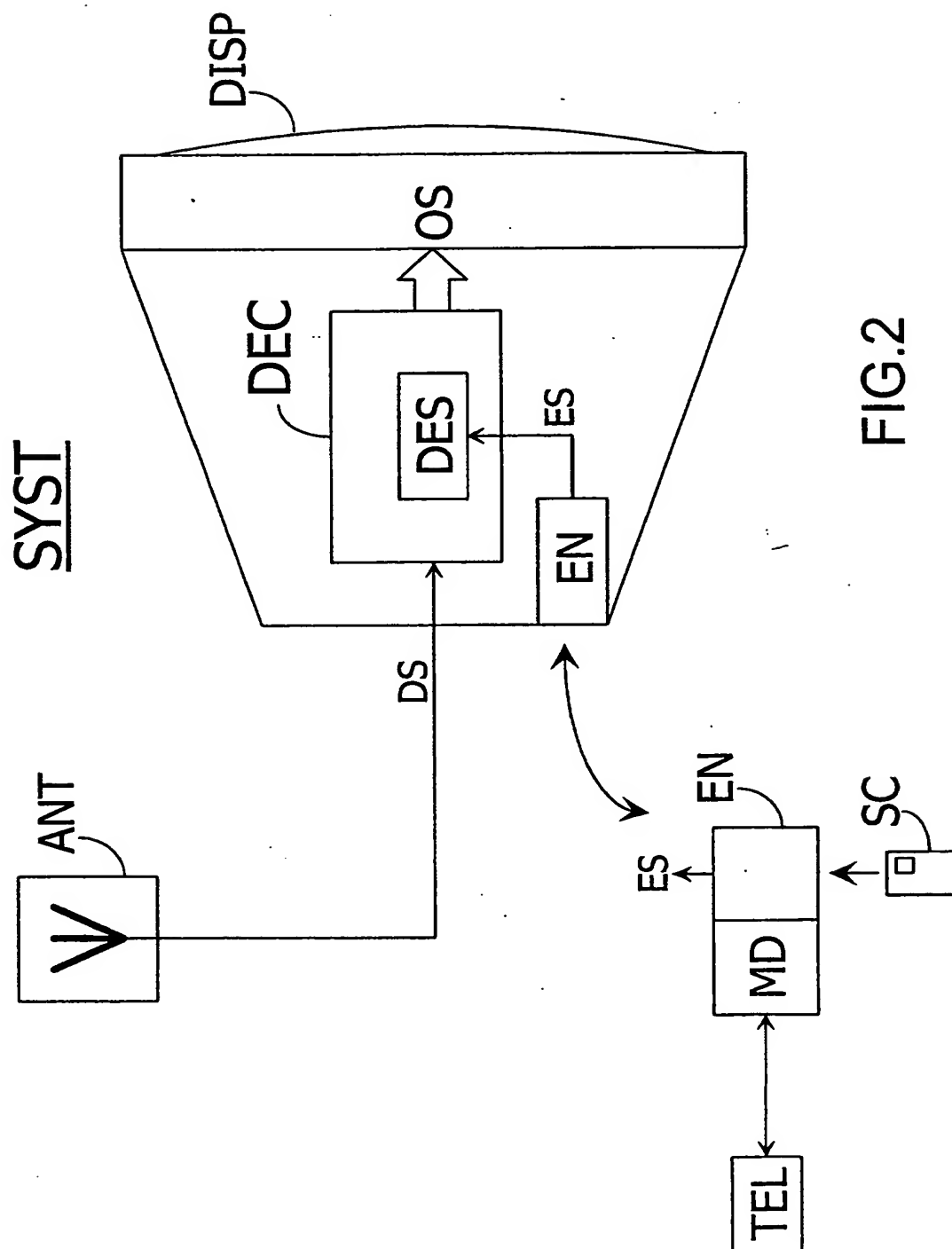


FIG.2

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

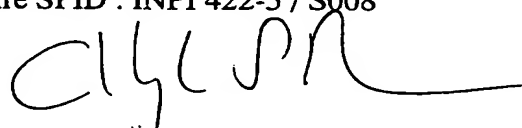
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° .. 1/ .. 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		PHFR010022	
N° D'ENREGISTREMENT NATIONAL		01 02 664	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Système de réception de signaux cryptés multi-opérateurs à encombrement et coût réduits			
LE(S) DEMANDEUR(S) :			
Koninklijke Philips Electronics N.V.			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		BENOIT	
Prénoms		Hervé	
Adresse	Rue	156 boulevard Haussmann	
	Code postal et ville	75008 PARIS	
Société d'appartenance (facultatif)		Société Civile SPID	
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Paris, le 27 février 2001 Christophe SAINT-MARC Mandataire SPID : INPI 422-5 / S008 	

This Page Blank (uspto)